On the Numbers of Lattice Points in the Square lxl+lyl≦u Satisfying $x+py \equiv O(mod q)$ (数論 : Diophantine Problem)

AUTHOR(S):

山本, 芳彦

CITATION:

山本, 芳彦. On the Numbers of Lattice Points in the Square lxl+lyl≦u Satisfying $x+py \equiv O(mod q)$ (数論 : Diophantine Problem). 数理解析研究所講究録 1978, 334: 91-97

ISSUE DATE:

1978-10

URL:

http://hdl.handle.net/2433/104185

数理解析研究所講究録
334巻 1978年 91-97

On the numbers of lattice points in the square $|x|+|y| \leqq u$ satisfying $x+py \equiv 0 \pmod{q}$

阪大 理　山本芳彦

今 q を与えられた正整数とし，p は q と互に素な整数とする．正整数 u に対して

$$(1) \qquad \begin{cases} |x|+|y| \leqq u \\ x+py \equiv 0 \pmod{q} \end{cases}$$

をみたす整数の組 $(x, y) \in \mathbb{Z}^2$ の個数を $a(u; p, q)$ と表わす．p' をもう一つの整数として，以後いつも $(p, q)=(p', q)=1$ と仮定する．もし p，p' が合同式 $p \equiv \pm p' \pmod{q}$ または $pp' \equiv \pm 1 \pmod{q}$ の一つをみたすならば，明らかに，すべての正整数 u に対して，$a(u; p, q) = a(u; p', q)$ となる．ここではこの逆も成立することを示す：

<u>定理1</u>．すべての正整数 u に対して，$a(u; p, q) = a(u; p', q)$ ならば，$p \equiv \pm p' \pmod{q}$ または $pp' \equiv \pm 1 \pmod{q}$ である．

この問題は微分幾何のある問題と関係していて，その一つの解答を与えるものである：いま，位数 g の巡回群を基本群にもつ3次元レンズ空間を考える．このとき，"そのリーマン多様体としての構造は Laplacian のスペクトルにより特徴付けられるか？" という問題が上記の整数論的問題に還えされるのである．g が特別な場合，$g = l^n$ または $g = 2l^n$ (l は素数)，には Ikeda-Yamamoto [1] により肯定的に解かれでいるが，定理1はそれが一般に肯定的であることを示している(c.f. [1], [2]).

整数の組 (x, y) が (1) をみたすとき，明らかに $(-x, -y)$ も (1) をみたすことより，

$$(2) \qquad \begin{cases} x \geq 0, \quad x + |y| = u \\ x + py \equiv 0 \pmod{g} \end{cases}$$

をみたす (x, y) の個数を $b(u; p, g)$ と表わすとき，定理1は次の定理と同値である．

<u>定理2</u>. すべての正整数 u に対して，$b(u; p, g) = b(u; p', g)$ ならば，$p \equiv \pm p' \pmod{g}$ または $pp' \equiv \pm 1 \pmod{g}$ である．

いま，$\zeta = e^{2\pi i/g}$ として，

$$F_j(X) = \frac{1}{(1-\zeta^j X)(1-\zeta^{pj}X)} + \frac{1}{(1-\zeta^j X)(1-\zeta^{-pj}X)}$$

$$G(X) = \sum_{j=0}^{g-1} F_j(X)$$

と定めると，$G(X)$ は X の有理関数であって，$b(u; p, g)$ の母関数となる，即ち $X = 0$ で

$$G(X) = 2g + g\sum_{u=1}^{\infty} X^{gu} + g\sum_{u=1}^{\infty} b(u; p, g) X^u$$

と展開される．p の代りに p' を用いて $G'(X)$ を同様に定義すれば，定理2は次の定理と同値になる．

定理3．$G(X) = G'(X)$ ならば $p \equiv \pm p' \pmod{g}$ または $pp' \equiv \pm 1 \pmod{g}$ である．

以下では定理3を証明する．

1. $G(X)$ の極と留数

$G(X)$ は $X = \zeta^k$ $(k = 0, 1, \cdots, g-1)$ のみ高々2位の極をもつ．特にそれが丁度2位の極となる必要十分条件は

$$k \equiv 0 \left(\mathrm{mod}\ \frac{g}{(p-1, g)}\right) \text{ または } k \equiv 0 \left(\mathrm{mod}\ \frac{g}{(p+1, g)}\right)$$

である．また1位の極ではその留数が

$$(3) \quad \frac{1}{1-\zeta^{-k(p-1)}} + \frac{1}{1-\zeta^{-k(s-1)}} + \frac{1}{1-\zeta^{k(p+1)}} + \frac{1}{1-\zeta^{k(s+1)}}$$

$$= 2 - \frac{1}{2} I_k$$

$$I_k = \cot\frac{(p-1)k\pi}{q} + \cot\frac{(s-1)k\pi}{q} - \cot\frac{(p+1)k\pi}{q} - \cot\frac{(s+1)k\pi}{q}$$

(ここで s は $ps \equiv 1 \pmod q$ をみたす整数) となる.
従って, $G(X) = G'(X)$ ならば $G(X)$ と $G'(X)$ は同じ極と同じ留数を持つことより, 必要なら p と $-p$ を交換することによって,

$$(4)\quad \begin{cases} (p-1, q) = (p'-1, q) = \varepsilon u_1 \\ (p+1, q) = (p'+1, q) = \varepsilon u_2 \\ q = \varepsilon u_1 u_2 r, \quad (u_1, u_2) = 1 \\ \varepsilon = (p-1, p+1, q) = 1 \text{ or } 2 \end{cases}$$

かつ

$$(5)\quad I_k = I'_k \quad (k \not\equiv 0 \pmod{u_1 r} \text{ かつ } k \not\equiv 0 \pmod{u_2 r})$$

を得る (ここで I'_k は p の代りに p' を用いて I_k と同様に定義したもの). s' を $p's' \equiv 1 \pmod q$ となる整数とし, $(p \pm 1, q) = (s \pm 1, q)$, $(p' \pm 1, q) = (s' \pm 1, q)$ となることより

$$\begin{cases} p-1 = \varepsilon u_1 a & p'-1 = \varepsilon u_1 a' \\ s-1 = \varepsilon u_1 b & s'-1 = \varepsilon u_1 b' \\ p+1 = \varepsilon u_2 c & p'+1 = \varepsilon u_2 c' \\ s+1 = \varepsilon u_2 d & s'+1 = \varepsilon u_2 d' \end{cases}$$

とおくと

$$I_k = \cot\frac{ak\pi}{u_2 r} + \cot\frac{bk\pi}{u_2 r} - \cot\frac{ck\pi}{u_1 r} - \cot\frac{dk\pi}{u_1 r}$$

$$I_k' = \cot\frac{a'k\pi}{u_2 r} + \cot\frac{b'k\pi}{u_2 r} - \cot\frac{c'k\pi}{u_1 r} - \cot\frac{d'k\pi}{u_1 r}$$

となる. ここで次の補題が重要である.

補題 (Chowla , Baker-Birch-Wirsing) $\frac{1}{2}\varphi(r)$個の値

$$\cot\frac{k\pi}{r} \quad ,\ (0<k<r/2 \text{ かつ } (k,r)=1)$$

は有理数体 $\mathbb{Q}$ 上一次独立である.

2. 定理の証明

定理3は次の場合に証明すれば十分であることがわかる.

(I) q = odd or $2\| q$; $u_1 = u_2 = 1$.

(II) (i) q = odd or $2\| q$; $u_1 \geq 3$.

(ii) $4\| q$; $u_1 \geq 3$.

(iii) $8 | q$; u_1 = even.

(III) $4\| q$; $u_1 = 2$, $u_2 = 1$.

Case(I): (5) において $k=1$ とすれば, 補題より容易に $p \equiv \pm p' \pmod q$ または $p \equiv \pm s' \pmod q$ を得る.

Case(II): k を (a) $k \equiv -1 \pmod{u_2 r}$, (b) $(k, q) = 1$, (c) $l | u_1$ かつ $l^e \| u_1 r$ (l は奇素数) に対して $k \not\equiv -1 \pmod{l^e}$ (d) ((iii)の場合のみ) $2^f \| u_1 r$ として $k \not\equiv -1 \pmod{2^f}$, をみたすように選んで, $I_k + I_1 = I_k' + I_1'$ となることより

$$(6)\qquad \cot\frac{c\pi}{u_{1r}}+\cot\frac{d\pi}{u_{1r}}+\cot\frac{ck\pi}{u_{1r}}+\cot\frac{dk\pi}{u_{1r}}$$
$$=\cot\frac{c'\pi}{u_{1r}}+\cot\frac{d'\pi}{u_{1r}}+\cot\frac{c'k\pi}{u_{1r}}+\cot\frac{d'k\pi}{u_{1r}}$$

となる．(6) に補題を適用して，起り得る一次従属関係を適当に場合分けして，$p\equiv p'$ または $p\equiv s'\pmod q$ を得る．

Case(Ⅲ)：このときも (Ⅱ) と同様で直接に補題を $I_h=I_h'$ には適用できないが，$I_1+I_{r+1}=I_1'+I_{r+1}'$ に対しては適用できることより (Ⅱ) と同様に $p\equiv p'$ または $p\equiv s'\pmod q$ を得る．

3. 注意（$L(1,\chi)\neq 0$ を用いない証明）

上記の証明では (Ⅰ),(Ⅱ),(Ⅲ) のいずれにおいても補題の使用が key point になっている．それはまた，Dirichlet の L 一関数において，$L(1,\chi)\neq 0$ であることに基づいているといってよい（c.f. [1] [2]）．しかし $q=l$（素数）の場合には，円分体 $\mathbb{Q}(\zeta)$ での素 ideal の分解：

$$(l)=(\lambda)^{l-1},\quad \lambda=1-\zeta$$

より，$\mathbb{Q}(\zeta)_{(\lambda)}$（$\lambda$ 一進体）においての $\dfrac{1}{1-\zeta^k}$ $(k=1,2,\cdots,q-1)$ の展開を考えることより $p\equiv\pm p'\pmod l$ または $pp'\equiv\pm 1\pmod l$ を直接に証明することができる（c.f. [2]）．

References

[1] A. Ikeda and Y. Yamamoto: On the spectra of 3-dimensional lens spaces (To appear)

[2] Y. Yamamoto: On the number of lattice points in the square $|x|+|y| \leq u$ with a certain congruence condition. (in preparation)

[3] A. Baker, B.J. Birch and E.A. Wirsing: On a Problem of Chowla, J. of Number Theory 5 (1973), 224-236.

[4] S. Chowla: The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, J. of Number Theory 2 (1970), 120-123.